SECURING THE SIGNAL

MITIGATION STRATEGIES TO STRENGTHEN CRISIS COMMUNICATION CHANNELS

CHRISTIAN STEINS

MAY 2025

IST Institute for SECURITY + TECHNOLOGY

Securing the Signal:
Mitigation Strategies to Strengthen Crisis Communication Channels

May 2025
Author: Christian Steins
Design: Sophia Mauro

IST

About the Institute for Security and Technology

Uniting technology and policy leaders to create actionable solutions to emerging security challenges

Technology has the potential to unlock greater knowledge, enhance our collective capabilities, and create new opportunities for growth and innovation. However, insecure, negligent, or exploitative technological advancements can threaten global security and stability. Anticipating these issues and guiding the development of trustworthy technology is essential to preserve what we all value.

The Institute for Security and Technology (IST), the 501(c)(3) critical action think tank, stands at the forefront of this imperative, uniting policymakers, technology experts, and industry leaders to identify and translate discourse into impact. We take collaborative action to advance national security and global stability through technology built on trust, guiding businesses and governments with hands-on expertise, in-depth analysis, and a global network.

We work across three analytical pillars: the **Future of Digital Security**, examining the systemic security risks of societal dependence on digital technologies; **Geopolitics of Technology**, anticipating the positive and negative security effects of emerging, disruptive technologies on the international balance of power, within states, and between governments and industries; and **Innovation and Catastrophic Risk**, providing deep technical and analytical expertise on technology-derived existential threats to society.

Learn more: https://securityandtechnology.org/

Contents

Summary

As global norms are challenged and emerging technologies accelerate, crisis communication systems between nuclear-armed states face urgent new threats. Designed to prevent escalation, these channels are increasingly vulnerable to both technical interference (e.g., cyber attacks, deepfakes) and diplomatic misuse (e.g., refusal to respond, use for coercion). This report identifies four critical scenarios and outlines a matched set of mitigation strategies designed to reinforce the reliability of crisis communications in high-stakes environments.

Introduction

Crisis communications channels, such as hotlines between heads of state or military leaders, have long played a vital role in diffusing nuclear risk.[1] Today, that role is more urgent than ever. The world is at an inflection point regarding a secure and peaceful future; the United Nations Disarmament Affairs Chief warned in 2023 that the current risk of nuclear weapons use is "higher than at any time since the Cold War."[2] The UN Common Agenda for Peace, released at the beginning of 2023, envisions improved collective security through open international cooperation and communication, among other methods.[3] Global leaders must heed its calls.

But real-world engagement is eroding. Diplomatic and crisis communication channels, designed to prevent conflict and clarify intentions, are increasingly susceptible to political manipulation and technical exploitation. Russia's withdrawal from arms control forums, China's refusal to respond after the 2023 U.S. surveillance balloon incident, and a growing reliance on ambiguous or coercive signals all reflect a dangerous trend: breakdowns in communication when it matters most.[4]

1 "Last Chance: Communicating at the Nuclear Brink," The Nautilus Institute, Stanley Center for Peace and Security, Institute for Security and Technology, May 14, 2020, https://securityandtechnology.org/virtual-library/reports/last-chance-communicating-at-the-nuclear-brink/.

2 "A New Nuclear Arms Race Looms," *The Economist*, August 29, 2023, https://www.economist.com/international/2023/08/29/a-new-nuclear-arms-race-looms; United Nations, "Risk of Nuclear Weapons Use Higher Than at Any Time Since Cold War, Disarmament Affairs Chief Warns Security Council," press release, March 31, 2023, https://press.un.org/en/2023/sc15250.doc.htm.

3 United Nations, "A New Agenda for Peace," July 2023, https://dppa.un.org/en/a-new-agenda-for-peace.

4 Geoff Brumfiel, "Russia is Scrapping its Ratification of a Key Nuclear Test Ban. Here's What That Means," *National Public Radio*, October 17, 2023, https://www.npr.org/2023/10/17/1206114320/russia-is-scrapping-its-ratification-of-a-key-nuclear-test-ban-heres-what-that-m; Isaac Chotiner, "What's Behind the Chinese Spy Balloon," *The New Yorker*, February 18, 2023, https://www.newyorker.com/news/q-and-a/whats-behind-the-chinese-spy-balloon.

Crisis communication failures may arise from deliberate refusals to engage, strategic misuse for coercive signaling, or attempts to exploit system vulnerabilities such as spoofing or network sabotage. These failures, whether driven by human decisions or infrastructural weaknesses, undermine the credibility and reliability of crisis communication channels, eroding a key safeguard against miscalculation and escalation during moments of heightened tension.[5]

Diplomatic and Technical Use Cases

This report highlights four key cases of crisis communication failure, divided into diplomatic misuse and technical exploitation. Diplomatic cases often involve the absence of established operational norms or the deliberate misuse of hotlines for the purpose of coercion or misinformation. In contrast, technical cases focus on how emerging threats, such as AI impersonation, authentication breaches, and cyber or electronic attacks, can compromise the reliability of communication systems. Together, these examples reveal the growing vulnerabilities facing nuclear and strategic crisis communications today.

Four Key Use Cases

This report considers two main categories of risk to crisis communication channels: diplomatic and technical. Each poses a unique challenge that undermines the core objective of preventing escalation during crises.

	Category	Case	Risk
	**Diplomatic**	Lack of signaling norms (e.g., misuse of deconfliction line in Syria)	Misinterpretation, escalation due to unclear protocols
	Diplomatic	Hotline used for threats or delay (e.g., China's conditional engagement)	Strategic silence or coercive signaling during crises
	**Technical**	AI impersonation and deepfakes (e.g., fake Kyiv mayor video)	False attribution leading to misinformed responses
	Technical	EMP or cyber attacks (e.g., potential crisis blackout via infrastructure sabotage)	Loss of functionality in critical moments

5 Alexa Wehsener and Sylvia Mishra, "Strengthening Resilience in 21st Century Crisis Communications," Institute for Security and Technology, July 2023, https://securityandtechnology.org/wp-content/uploads/2023/07/Strengthening-Resilience-in-21st-Century-Crisis-Communications.pdf.

The following diplomatic and technical case studies illustrate these risks in detail and inform the mitigation strategies proposed later in this report.

Case Studies of Diplomatic Risk

Absence of Signaling Norms and Operational Protocols: United States-Russia Deconfliction Line in Syria

One of the most dangerous failures in diplomatic crisis communication is the absence of clear signaling norms and shared expectations for hotline use.[6] The deconfliction line between US and Russian forces in Syria initially functioned as intended, facilitating real-time coordination in a complex battlespace.[7] However, over time, Russia began using the line not for coordination but to issue ambiguous threats, undermining trust and causing each side to question the sincerity of messages communicated via this channel. This breakdown culminated in a deadly clash when Russia sent a warning to vacate a U.S.-held position in advance of an attack, and the US responded that it was holding its position. Russia misread US intent and proceeded with the attack, resulting in dozens of Russian casualties.[8] The incident underscores that technical functionality alone is not enough—hotlines must be underpinned by credible, mutually understood protocols to prevent dangerous miscalculation.

Crisis Hotlines Used for Coercion and Strategic Delay: China's Conditional Engagement

Crisis communication channels are sometimes misused not for de-escalation, but to assert dominance, delay dialogue, or issue veiled threats—actions rooted in a lack of political will or deliberate diplomatic manipulation. A telling example comes from China's recent working paper on nuclear risk reduction, which supports improved communication only after broader security conditions improve.[9] This argument, echoed by Russia, effectively stalls engagement while preserving strategic ambiguity.[10] This logic allows states to avoid accountability and

6 Leah Walker and Alexa Wehsener, "To the Point of Failure: Identifying Failure Points for Crisis Communications Systems," Institute for Security and Technology, November 2022, https://securityandtechnology.org/virtual-library/reports/to-the-point-of-failure-identifying-failure-points-for-crisis-communications-systems/.

7 Juliette Faure, "The US-Russia Military Hotline in Europe: Key Principles for Risk Reduction," European Leadership Network, March 17, 2022, https://europeanleadershipnetwork.org/commentary/the-us-russia-military-hotline-in-europe-key-principles-for-risk-reduction-from-the-us-russia-deconfliction-measures-in-syria/.

8 Andrew S. Weiss and Nicole Ng, "Collision Avoidance: The Lessons of U.S. and Russian Operations in Syria," Carnegie Endowment for International Peace, March 20, 2019, https://carnegieendowment.org/research/2019/03/collision-avoidance-the-lessons-of-us-and-russian-operations-in-syria.

9 "Working Paper on Nuclear Risk Reduction submitted by China to the Preparatory Committee for the 2026 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons," Ministry of Foreign Affairs, The People's Republic of China, August 8, 2023, https://www.mfa.gov.cn/eng/wjb/zzjg_663340/jks_665232/kjfywj_665252/202406/t20240606_11405415.html.

10 Guy Faulconbridge and Lidia Kelly, "Russia Says Emergency Hotlines with US and NATO Remain as Nuclear Risks Rise," *Reuters*, October 8, 2024, https://www.reuters.com/world/europe/russia-says-emergency-hotlines-with-us-nato-remain-nuclear-risks-rise-2024-10-08/.

exploit silence as a tool of coercion, feeding a cycle of mistrust and instability. When crisis hotlines are used for posturing rather than clarification, they can exacerbate misperceptions rather than reduce them. This case highlights the urgent need for credible, mutually agreed-upon norms governing the responsible use of these systems.

Case Studies of Technical Risk

AI-Driven Impersonation and Deepfake Threats

Advances in artificial intelligence and synthetic media have introduced a critical vulnerability to crisis communications:[11] the potential for malicious actors to impersonate world leaders through deepfake audio or video.[12] While initially used for fraud and social engineering, these tools now pose serious risks to diplomatic networks. The synthetic media's ability to appear real is rapidly improving, and in high-pressure crisis settings where speed can outweigh caution, even a convincing fake could trigger a strategic or military response. Recent incidents, including fake video calls with European officials and AI-generated impersonations of heads of state, reveal how easily trust in secure communications can be eroded.[13] These are not isolated events but early warnings of a broader threat. As synthetic media becomes more sophisticated, governments must treat the risk of impersonation not as hypothetical but as a strategic challenge requiring robust verification protocols.

EMP and Cyber Attacks on Crisis Infrastructure

Electronic warfare and cyber operations pose a severe threat to crisis communication systems, aiming not to deceive but to disable or destroy them at critical moments. Among the most dangerous are electromagnetic pulse (EMP) attacks—triggered by nuclear or non-nuclear means—which can silently cripple electronic infrastructure including secure diplomatic and military networks.[14] While once seen as hypothetical, non-nuclear EMP weapons are now operational in multiple states and could be used early in a conflict to paralyze communications. At the same time, cyber threats, from ransomware to sophisticated state-sponsored sabotage, remain a constant risk, as demonstrated in recent conflicts. These attacks blur the line between technical disruption and acts of war, especially given

11 IEEE Public Safety Technology, "Biometric Authentication Technologies for First Responders," last accessed May, 2025, https://publicsafety.ieee.org/topics/biometric-authentication-technologies-for-first-responders.

12 Leah Walker, "Playing Telephone: Hoax Calls and the Insecurity of Leader to Leader Communications," Institute for Security and Technology, July 2022, https://securityandtechnology.org/wp-content/uploads/2023/03/Playing-Telephone-Hoax-Calls-and-the-Insecurity-of-Leader-to-Leader-Communications.pdf.

13 Sasha Shilina, "Biometrics: A Beacon of Trust in the Digital Media Crisis," April 18, 2024, https://medium.com/@sshshln/biometrics-a-beacon-of-trust-in-the-digital-media-crisis-10f13ebe81d5.

14 Katherine Schmidt, "Effects of Electromagnetic Pulses on Communication Infrastructure," Institute for Security and Technology, January 2024, https://securityandtechnology.org/virtual-library/reports/effects-of-electromagnetic-pulses-on-communication-infrastructure/.

their often ambiguous attribution.[15] Without hardening against EMP and cyber threats, crisis communication systems cannot be trusted to function when needed most, making technical and diplomatic countermeasures an urgent priority.

Risk Mitigation Strategies for Crisis Communication

To address the vulnerabilities discussed in the above use cases, this report proposes four corresponding mitigation strategies:

- **Diplomatic tools** include norm-setting and confidence-building measures (CBMs).
- **Technical solutions** focus on EMP resilience and verification protocols.

Strategy	Addresses	Example Actions
Shared Norms for Hotline Use	Diplomatic misuse (threats, silence)	Create voluntary principles and operating norms for hotline use
EMP-Hardened Mesh Networks	EMP and cyber sabotage	Deploy resilient nodes with satellite links and hardened circuits
Biometric Verification	AI/deepfake impersonation	Fingerprint, iris, or voiceprint authentication on crisis devices

Diplomatic Mitigation Strategies

Establishing Norms and Guidelines for Responsible Use

To mitigate the risks of diplomatic misuse, states must move beyond informal norms and establish shared principles governing the use of crisis communication channels. This strategy calls for convening a neutral, multilateral working group to draft voluntary but politically meaningful standards, including commitments to 24/7 responsiveness, non-escalatory messaging, and clear authentication protocols. Forums such as the Munich Security Conference, the Shangri-La Dialogue,[16] or the NPT PrepCom could host side panels to launch this dialogue, ideally involving both nuclear and non-nuclear states, as well as technical experts. While consensus may be difficult due to differing threat perceptions and political

15 Rebecca Hersman, "Wormhole Escalation in the Nuclear Age," *Texas National Security Review* 3 (no. 3), Autumn 2020, https://tnsr.org/wp-content/uploads/2020/07/06_TNSR-Journal-Vol-3-Issue-3-Hersman.pdf.

16 "IISS Shangri-La Dialogue," Institute for International and Strategic Studies, last accessed May 2025, https://www.iiss.org/events/iiss-shangri-la-dialogue/.

dynamics, a tiered, evolving framework of best practices offers a flexible path forward.[17] The goal is not new treaties, but credible, shared expectations that strengthen the integrity of communication during crises.

Confidence-Building Measures to Sustain Readiness and Trust

Confidence-building measures (CBMs) enhance crisis communication by normalizing its use, fostering trust, and linking messages to verifiable actions.[18] These channels should be exercised regularly to ensure they remain functional and familiar, using best practices such as the daily exchanges by the US-Russia National and Nuclear Risk Reduction Center (NNRRC). CBMs can also tie communication systems to event notifications, such as missile test alerts, to prevent misinterpretation and offer strategic reassurance.[19] Moving from bilateral to multilateral frameworks could further enhance transparency and stability among nuclear-armed states. While not a cure-all, CBMs bridge the gap between diplomatic intent and technical systems, making crisis communications more credible, dependable, and trusted when it matters most.

Technical Mitigation Strategies

Building an EMP-Hardened, Global Mesh Network

To address the threat of EMP attacks and electronic sabotage, crisis communication systems must evolve beyond fragile bilateral arrangements toward a hardened, multilateral infrastructure. A global mesh network, built on a redundant and distributed architecture, would enable secure communication even under degraded conditions, such as nuclear detonations or cyber attacks. This system would utilize a combination of satellite links, low-bandwidth relays, and terrestrial nodes that can operate independently of GPS or the internet. Rather than replacing existing hotlines, it would act as a resilient overlay, ensuring continuity of dialogue when traditional channels fail. Its success depends on rigorous technical standards and sustained international cooperation to guarantee interoperability, security, and trust during moments of extreme tension.

Integrating Biometric Verification into Crisis Protocols

Biometric verification should be integrated into crisis communication protocols to guard against impersonation threats, particularly those enabled by AI-generated deepfakes.[20] Each

17 Christian Steins, "The South Korea-Japan-United States Trilateral Hotline: A Reminder of the Importance of Crisis Communications," Institute for Security and Technology, January 18, 2024, https://securityandtechnology.org/blog/the-south-korea-japan-united-states-trilateral-hotline/.

18 Alexa Wehsener, Andrew W. Reddie, Leah Walker, Philip Reiner, "AI-NC3 Integration in an Adversarial Context: Strategic Stability Risks and Confidence Building Measures," Institute for Security and Technology, February 2023, https://securityandtechnology.org/wp-content/uploads/2023/02/AI-NC3-Integration-in-an-Adversarial-Context.pdf.

19 Timothy Wright, "Challenges to Multilateral Arms Control," International Institute for Strategic Studies, October 6, 2024, https://www.iiss.org/online-analysis/missile-dialogue-initiative/2023/10/challenges-to-multilateral-arms-control/.

20 Original insights into biometrics gained from a conversation with Dr. Olamide Samuel in London, U.K., August 2024.

endpoint device would authenticate the sender through biometric scans such as voiceprint, fingerprint, retinal, or facial recognition, ensuring that only verified users can transmit critical messages.[21] A flexible system would accommodate varying national standards, allowing for single or multi-factor authentication. Verification would occur during secure handoffs and could include preset signal codes linked to specific messages (e.g., "No launch detected"), reducing ambiguity in high-pressure situations.[22] While technically complex, biometric validation offers a direct and necessary solution to the growing risk of false attribution in crisis communications.

BIOMETRIC COMPARISON TABLE: BIOMETRIC VERIFICATION SYSTEMS

The table below presents an analysis of the strengths and risks associated with the various types of biometric verification technologies. The Security Level assesses each technology's relative strength in assuring the identity of users. Cross-State Viability compares the level of difficulty in integrating these verification measures across different states. The final column considers the relative level of risk that each technology could be misused by bad actors, with high risk indicating that the technology is easier to exploit or misuse.

Biometric Type	Security Level	Cross-State Viability	Risk of Misuse
Voiceprint	Medium	High	High
Retinal/Iris Scan	High	Medium	Low
Fingerprint Scan	Medium - High	High	Medium - Low
Facial Recognition	Medium	Medium	Medium

Tradeoffs and Considerations

Every mitigation strategy carries tradeoffs. Technical upgrades demand funding, diplomatic progress requires patience, and agreement among strategic rivals will always be fragile. But the cost of failure, whether a failed message in a moment of crisis or a misinterpreted signal with nuclear implications, is far greater. The value of these systems is not only in their technical design, but in the trust they represent and the restraint they enable. Policymakers must weigh these tradeoffs carefully to ensure solutions do not create new vulnerabilities or geopolitical friction.

21 Hanna Skryl, "Contactless Biometric Identification in 2022," Vilmate, last accessed May 2025, https://vilmate.com/blog/contactless-biometric-identification/.

22 "Why Veriff?" Veriff, last accessed May 2025, https://www.veriff.com/about/why-veriff.

Diplomatic Mitigation Strategy

Norms & Standards

Tradeoff

Slow progress due to geopolitical mistrust

Considerations

Establishing shared communication protocols depends on trust, compromise, and sustained diplomatic engagement. In contentious environments, such efforts risk being delayed, manipulated, or deadlocked, particularly when adversaries weaponize ambiguity.

Diplomatic Mitigation Strategy

CBMs

Tradeoff

Possible exposure of sensitive military activity

Considerations

CBMs promote routine communication and transparency but may be seen as exposing sensitive capabilities. States must balance concerns over deterrence with the urgent need to prevent misinterpretation in moments of crisis.

Technical Mitigation Strategy

EMP-Hardened Mesh Networks

Tradeoff

High infrastructure cost; could be seen as escalatory

Considerations

Building resilient infrastructure through hardened nodes and distributed networks requires significant investment and coordination. In some contexts, such developments could be perceived as escalatory or dual-use, complicating diplomatic signaling.

Technical Mitigation Strategy

Biometric Verification

Tradeoff

Privacy and political resistance; interoperability issues

Considerations

While biometric systems offer robust protection against impersonation, they raise concerns about privacy, data security, and political acceptability, particularly in states with limited transparency. Mutual authentication protocols may be viewed as intrusive, deterring adoption in adversarial or asymmetrical relationships.

Conclusion: Reinforcing Communication in an Age of Strategic Uncertainty

This report has identified four critical vulnerabilities, two diplomatic and two technical, and proposed corresponding mitigation strategies designed to reduce the likelihood of catastrophic misunderstanding. EMP hardening and mesh network deployment, as well as biometric authentication, would help reduce technical risk. Norm-setting, confidence-building, and institutionalizing responsible use would mitigate diplomatic vulnerabilities. These recommendations aim not to overreach but to reinforce, offering a layered approach to risk reduction rooted in realism and focused on resilience.

Crisis communication channels remain vital for preventing escalation during moments of tension, but they now face increasingly sophisticated threats that are no longer hypothetical. Preserving peace in today's complex and contested environment requires reinforcing and adapting existing systems to meet emerging and anticipated challenges. With strategic investment, diplomatic coordination, and the will to act before crises unfold, states can ensure these channels remain trusted, resilient, and ready when they are needed most.

INSTITUTE FOR SECURITY AND TECHNOLOGY

www.securityandtechnology.org

info@securityandtechnology.org